The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

1/14/2014

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB14-02)

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow an attacker to take control of the affected system. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE:

At this time these vulnerabilities are not publicly disclosed and there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- Adobe Flash Player 11.9.900.170 and earlier versions for Windows and Macintosh
- Adobe Flash Player 11.2.202.332 and earlier versions for Linux
- Adobe AIR 3.9.0.1380 and earlier versions for Windows and Macintosh
- Adobe AIR 3.9.0.1380 and earlier versions for Android
- Adobe AIR 3.9.0.1380 SDK and earlier versions
- Adobe AIR 3.9.0.1380 SDK & Compiler and earlier versions

RISK:

Government:

- Large and medium government entities: High
- Small government entities: High

Businesses:

- Large and medium business entities: High
- Small business entities: High

Home users: Hig:

TECHNICAL SUMMARY:

Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. Specifically, the vulnerabilities identified may allow an attacker to bypass Flash Player security protections or defeat memory address layout randomization in such a way that results in remote code execution. Failed exploitation attempts may cause denial-of-service conditions. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Adobe:

http://helpx.adobe.com/security/products/flash-player/apsb14-02.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0491

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0492